the answer in the determination action **812** is no, the data recoverability time span has not expired, flow proceeds to the determination action **816**.

**[0223]** In the determination action **816**, the storage system determines whether a request has been received, to cancel deletion of data or undelete data. This could be an explicit request from a tenant, or a notification from a storage or service provider, etc. If the answer is no, no such request has been received, flow proceeds back to the determination action **812**, to continue monitoring for requests within the data recoverability time span. If the answer is yes, a request has been received to cancel deletion of data or undelete data, flow proceeds to the action **818**. In the action **818**, the storage system imports the key from the tenant. The imported key should be the key that was exported in the action **806**. In an action **820**, the storage system supports access to the data by the tenant using the key. Doing so fulfills the request to cancel deletion of data, or undelete data, as received and determined for the action **816**.

**[0224]** FIG. **9** is a flow diagram of a method for secure data deletion and undeletion in a multitenant environment, which can be performed by embodiments of a storage system depicted in FIGS. **4** and **6**, and variations thereof. The method can be performed by one or more processors in a storage system. In an action **902**, the storage system stores encrypted data from multiple tenants in the storage system as a multitenant environment. As in other embodiments, the storage system has specific keys for specific tenants, encrypts data of a tenant with a key associated to the tenant, etc.

**[0225]** In an action **904**, the storage system receives a request from the tenant to delete data. As in other embodiments, this request could be an explicit request from the tenant, or inferred from a notification from the tenant, a storage provider or service provider, etc. In an action **906**, the storage system exports the key to the tenant. The exported key is the key used in the storage system for encryption and decryption of the tenant data. In an action **908**, the key is retained in the storage system as a master key for approval. For example, the key could be retained in a master key repository, but not in active use for data accesses, so that the data that is requested to be deleted is then inaccessible.

**[0226]** In an action **910** of FIG. **9**, the storage system starts a data recoverability time span. Mechanisms for this action **910** are discussed above, and applicable to any embodiment that has a data recoverability time span. It should be appreciated that action **910** may start after action **904** in some embodiments. In a determination action **912**, the storage system determines whether the tenant returns the key, within the data recoverability time span. If the determination is no, the tenant has not returned the key within the data recoverability time span, flow proceeds to the action **918**, to delete the master key in the storage system. If the determination is yes, the tenant has returned the key within the data recoverability time span, flow proceeds to the determination action **914**. In the determination action **914**, the storage system determines whether the returned key is approved with the master key. Approval with the master key can be performed as described above in reference to FIG. **6**, for example by comparing the returned key and the master key. If the determination is no, the returned key is not approved with the master key, flow proceeds back to the determination action **912**, to continue monitoring for return of the key and the data recoverability time span. If the determination is yes, the returned key is approved with the master key (and the key was returned by the tenant within the data recoverability time span), flow proceeds to the action **916**. In the action **916**, the storage system supports access to the data by the tenant, using the key. This fulfills the request to undelete the data, as inferred from the return of the key.

**[0227]** Advantages and features of the present disclosure can be further described by the following statements:

**[0228]** 1. A method of secure data deletion in a multitenant environment, performed by a storage system, comprising:

**[0229]** associating a key with a tenant, in the multitenant environment, as a result of the storage system receiving data from the tenant through a virtual local area network (VLAN) or from an Internet protocol (IP) address;

**[0230]** storing the data, encrypted by the key, in the storage system; and

**[0231]** determining that the key, as retained in the storage system, is to be deleted, so that the data is to be inaccessible in unencrypted form, responsive to a request from the tenant to delete the data.

**[0232]** 2. The method of statement **1** wherein/further comprising tagging the key with a tenant tag.

**[0233]** 3. The method of statement **2** or statement **1** wherein/further comprising deleting the key, after a data recoverability time span.

**[0234]** 4. The method of statement **3**, statement **2**, or statement **1** wherein/further comprising canceling a direction to delete the key, responsive to a request from the tenant to cancel deleting the data.

What is claimed is:

**1**. A method for secure data deletion in a multitenant environment, performed by a storage system, comprising:

associating a key with a tenant, in the multitenant environment, as a result of the storage system receiving data from the tenant through a virtual local area network (VLAN) or from an Internet protocol (IP) address;

storing the data, encrypted by the key, in the storage system; and

determining that the key, as retained in the storage system, is to be deleted, so that the data is to be inaccessible in unencrypted form, responsive to a request from the tenant to delete the data.

**2**. The method for secure data deletion in a multitenant environment, performed by a storage system, of claim **1** wherein the associating the key with the tenant comprises:

tagging the key with a tenant tag.

**3**. The method for secure data deletion in a multitenant environment, performed by a storage system, of claim **1** further comprising:

deleting the key, after a data recoverability time span.

**4**. The method for secure data deletion in a multitenant environment, performed by a storage system, of claim **1** further comprising:

canceling a direction to delete the key, responsive to a request from the tenant to cancel deleting the data.

**5**. The method for secure data deletion in a multitenant environment, performed by a storage system, of claim **1** further comprising:

excluding the encrypted data from garbage collection, during a data recoverability time span.